CHELO HISPANA, S.L.

DOCUMENTO DE SEGURIDAD
NIVEL BÁSICO

DENOMINACIÓN SOCIAL	**CHELO HISPANA, S.L.**
DOMICILIO SOCIAL	**C/ SIERRA DE ARAS, 9 LUCENA 14900 (CORDOBA)**
C.I.F./N.I.F.	**B14620108**
ACTIVIDAD	**RESTO EMPRESARIALES-ALQUILER DE COCHES**
FECHA EXPEDICIÓN:	**05/05/2016**

DOCUMENTOS, ANEXOS Y CONTRATOS IMPLANTACIÓN LEY ORGÁNICA PROTECCIÓN DATOS DE CARÁCTER PERSONAL

1.- DOCUMENTO DE SEGURIDAD

A).- HOJAS DE REGISTRO

- INCIDENCIAS
- AUTORIZACIONES
- ACCESO DOCUMENTACIÓN
- ENTRADA DE SOPORTES
- SALIDA DE SOPORTES

B).- ANEXOS:

- **EQUIPOS:** HACE REFERENCIA A LOS EQUIPOS INFORMATICOS QUE SE TIENEN EN LA EMPRESA (MARCA, MODELO, CARACTERÍSTICAS)
- **PROGRAMAS:** HACE REFERENCIA A LOS PROGRAMAS UTILIZADOS EN LA EMPRESA.
- **ENCARGADOS:** HACE REFERENCIA A OTRAS EMPRESAS QUE NOS PRESTAN ALGÚN SERVICIO EL CUAL IMPLICA ACCESO A DATOS DE CARÁCTER PERSONAL.
- **ENCARGOS:** HACE REFERENCIA A AQUELLAS EMPRESAS RESPECTO DE LAS CUALES NUESTRA EMPRESA TRABAJA CON DATOS DE CARÁCTER PERSONAL DE LAS MISMAS.
- **USUARIOS:** HACE REFERENCIA A LOS TRABAJADORES DE LA EMPRESA QUE TIENEN ACCESO A DATOS DE CARÁCTER PERSONAL.
- **SOPORTES:** HACE REFERENCIA A LA FORMA EN QUE ESTA GUARDADOS EN LA EMPRESA LOS DATOS DE CARÁCTER PERSONAL.

C).- FORMULARIOS DE DERECHOS

2.- FUNCIONES Y OBLIGACIONES DEL PERSONAL

3.- CONTRATOS ENCARGADOS DEL TRATAMIENTO: HACE REFERENCIA A AQUELLOS CONTRATOS CON LAS EMPRESAS QUE NOS PRESTAN SERVICIOS Y QUE TIENEN ACCESO A DATOS DE NUESTROS CLIENTES, PROVEEDORES, EMPLEADOS, O CUALQUIER OTRO.

4.- CONTRATO SIN ACCESO A DATOS: HACE REFERENCIA AL CONTRATO FIRMADO CON AQUELLAS EMPRESAS QUE NOS PRESTAN ALGÚN SERVICIO PERO QUE EL MISMO NO IMPLICA EL ACCESO A DATOS DE CARÁCTER PERSONAL.

5.- NOTIFICACION DE FICHEROS: HACE REFERENCIA A LOS FICHEROS QUE TENEMOS EN LA EMPRESA CON DATOS DE CARÁCTER PERSONAL Y QUE HEMOS NOTIFICADO A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

ÍNDICE

CONTENIDO DEL DOCUMENTO DE SEGURIDAD

ÍNDICE

CONTENIDO DEL DOCUMENTO DE SEGURIDAD

OBJETO DEL DOCUMENTO

En virtud de lo establecido en el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, "LOPD"), el Responsable de los Ficheros[1] y, en su caso, el Encargado del Tratamiento[2] deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal, a los efectos de evitar e impedir su alteración, pérdida, tratamiento o acceso no autorizados.

Las medidas necesarias para garantizar la seguridad de dichos datos se establecen en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, "Reglamento de Protección de Datos" o "R.D. 1720/2007"). En dicho Real Decreto se establece la obligación de que aquellas personas físicas o jurídicas que dispongan de ficheros con datos de carácter personal elaboren un documento en el cual se detallen las medidas de seguridad necesarias para garantizar la confidencialidad de dichos datos (en adelante, "Documento de Seguridad").

El objeto del presente Documento de Seguridad es, por tanto, establecer las medidas de índole técnica y organizativas necesarias para garantizar los niveles de seguridad que deben reunir todos los ficheros con datos de carácter personal titularidad de **CHELO HISPANA, S.L.** (en adelante, "la Empresa" o "el Responsable de los Ficheros"), así como los centros de tratamiento, los locales, los equipos, los sistemas, los programas y las personas vinculadas a la Empresa que intervengan en el tratamiento de los datos de carácter personal sujetos al régimen de la LOPD.

Mediante el presente Documento, el Responsable de los Ficheros establece, elabora e implanta la normativa de seguridad de obligado cumplimiento para el personal de **CHELO HISPANA, S.L.** con acceso a los datos de carácter personal y a los sistemas de información. En este sentido, en el presente Documento de Seguridad quedarán definidas las funciones y obligaciones de cada uno de los usuarios con acceso a los datos de carácter personal y a los sistemas de información.

---

[1] ***Responsable del fichero o tratamiento:*** *Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.*

[2] ***Encargado del tratamiento:*** *La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.*

Será responsabilidad del Responsable de los Ficheros adoptar las medidas necesarias para que el personal de la Empresa conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento. En el presente Documento se establece el contenido que deberá facilitarse al personal con acceso a datos personales, así como el procedimiento para informarles.

DEFINICIONES

Los siguientes términos y expresiones, a efectos del presente Documento de Seguridad y según lo previsto en la LOPD y en el R.D. 1720/2007, tendrán el siguiente significado.

1. Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

2. Persona identificable: Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

3. Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

4. Fichero no automatizado: Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

5. Tratamiento de datos: Cualquier operación o procedimiento técnico, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

6. Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

7. Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

8. Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

9. Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

10. Destinatario o cesionario: La persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

11. Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

12. Dato disociado: Aquél que no permite la identificación de un afectado o interesado.

DEFINICIONES

13. Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

14. Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

15. Exportador de datos personales: La persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice una transferencia de datos de carácter personal a un país tercero.

16. Importador de datos personales: La persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

17. Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, las guías de servicios de comunicaciones electrónicas y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

18. Sistemas de información: Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

19.Usuario: Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

20. Perfil de usuario: Accesos autorizados a un grupo de usuarios.

21. Accesos autorizados: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

22. Recurso: Cualquier parte componente de un sistema de información.

DEFINICIONES

23. Identificación: Procedimiento de reconocimiento de la identidad de un usuario.

24. Autenticación: Procedimiento de comprobación de la identidad de un usuario.

25. Control de acceso: Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

26. Contraseña: Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

27. Incidencia: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

28. Soporte: Objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

29. Documento: Todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

30. Ficheros temporales: Ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

31. Transmisión de documentos: Cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

32. Copia del respaldo: Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación

33. Responsable de seguridad: Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

RESPONSABLES

Cumpliendo con la obligación legal determinada en el artículo 88 del R.D. 1720/2007, **CHELO HISPANA, S.L.** en calidad de Responsable de los Ficheros y/o de Encargado del Tratamiento, ha elaborado el presente Documento de Seguridad.

Será responsabilidad de ambos, del Responsable de los Ficheros y del Responsable de Seguridad, mantener el presente Documento debidamente actualizado y conforme a la legislación y normativa aplicable en cada momento.

Responsable de los Ficheros
CHELO HISPANA, S.L.

ÁMBITO DE APLICACIÓN

El presente Documento de Seguridad será de aplicación a la totalidad de documentos, soportes y sistemas de información de ***CHELO HISPANA, S.L.*** que almacenen o traten datos de carácter personal. Dichos sistemas de información están constituidos por los siguientes recursos:

a) Conjunto de ficheros, automatizados y no automatizados, titularidad de ***CHELO HISPANA, S.L.*** que contengan datos de carácter personal.

b) Conjunto de ficheros, automatizados y no automatizados, cuyo tratamiento sea realizado por ***CHELO HISPANA, S.L.*** en calidad de Encargado del Tratamiento.

c) Equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

d) Programas informáticos de que disponga ***CHELO HISPANA, S.L.*** para el tratamiento o almacenamiento de los datos de carácter personal.

e) Soportes informáticos utilizados por ***CHELO HISPANA, S.L.*** para el almacenamiento de datos de carácter personal.

A continuación se describen los recursos utilizados por ***CHELO HISPANA, S.L.***:

I. FICHEROS

CHELO HISPANA, S.L. es responsable de distintos ficheros con datos de carácter personal. La relación y estructura de dichos ficheros titularidad de ***CHELO HISPANA, S.L.*** se detalla en el **Anexo I** al presente Documento de Seguridad.

Asimismo, ***CHELO HISPANA, S.L.*** puede realizar el tratamiento de distintos ficheros con datos de carácter personal en calidad de Encargado del Tratamiento. La relación de los ficheros tratados por parte de ***CHELO HISPANA, S.L.*** en calidad de Encargado del Tratamiento y cuyo tratamiento se realiza en los propios locales de la Empresa se detallan en el **Anexo II** al presente Documento de Seguridad.

II. EQUIPOS

CHELO HISPANA, S.L. dispone de distintos equipos mediante los cuales se tratan o almacenan datos de carácter personal. Se adjunta como **Anexo III** al presente Documento de Seguridad, la relación de equipos utilizados por ***CHELO HISPANA, S.L.*** que tratan o almacenan datos de carácter personal.

III. PROGRAMAS INFORMÁTICOS

CHELO HISPANA, S.L. dispone de diferentes programas informáticos mediante los cuales se tratan o almacenan datos de carácter personal. Se adjunta como **Anexo IV** al presente Documento de Seguridad, la relación de programas o aplicaciones informáticas utilizadas por ***CHELO HISPANA, S.L.*** que tratan o almacenan datos de carácter personal.

IV. SOPORTES INFORMÁTICOS

CHELO HISPANA, S.L. utiliza diferentes soportes informáticos para almacenar datos de carácter personal. Se adjunta como Anexo V al presente Documento de Seguridad, la relación de soportes que almacenan datos de carácter personal utilizados por ***CHELO HISPANA, S.L.***

NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

Para garantizar la seguridad de los sistemas de información de ***CHELO HISPANA, S.L.*** y de cada uno de sus recursos, se establecen las siguientes medidas, normas, procedimientos, reglas y estándares de seguridad. El Responsable de los Ficheros procederá en todo momento siguiendo las medidas que a continuación se detallan y, en su caso, deberá informar a los diferentes miembros de ***CHELO HISPANA, S.L.*** que, en virtud de sus funciones o responsabilidades, traten datos de carácter personal.

I. IDENTIFICACIÓN Y AUTENTICACIÓN

El Responsable de los Ficheros deberá establecer un sistema que permita la identificación, de forma inequívoca y personalizada, de todo aquel usuario que intente acceder a los sistemas de información, así como la verificación de que está autorizado, para permitirle, en su caso, el acceso a los datos personales.

El Responsable de los Ficheros será el encargado de que exista una relación actualizada de usuarios*** que tengan acceso autorizado a los sistemas de información y de establecer procedimientos de identificación**** y autenticación***** para dicho acceso.

En el **Anexo VI** al presente Documento de Seguridad se relacionan los usuarios autorizados a acceder a los documentos y sistemas de información de ***CHELO HISPANA, S.L.*** que contengan datos de carácter personal.

CONTRASEÑAS:

Cuando el mecanismo de autenticación se base en el uso de contraseñas******, existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. Las contraseñas se modificarán con una periodicidad máxima de un año. Mientras estén vigentes, las contraseñas se almacenarán de forma ininteligible.

Se adjunta como **Anexo VII** al presente Documento de Seguridad, los procedimientos de identificación y autenticación establecidos por ***CHELO HISPANA, S.L..***

***Usuario:** *Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.*

****Identificación:** *Procedimiento de reconocimiento de la identidad de un usuario.*

*****Autenticación:** *Procedimiento de comprobación de la identidad de un usuario.*

******Contraseña:** *Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.*

El Responsable de los Ficheros se encargará en todo momento de mantener actualizada la información contenida en dichos Anexos.

II. CONTROL DE ACCESOS

Se establece como medida de seguridad que los usuarios tendrán acceso autorizado únicamente a aquellos datos personales y recursos que precisen para el desarrollo de sus funciones, en virtud de su puesto de trabajo y cargo. Se deberá disponer en todo momento de los sistemas necesarios de seguridad físicos y lógicos para restringir dichos accesos.

El Responsable de los Ficheros establecerá los mecanismos oportunos para evitar que un usuario pueda acceder a datos de carácter personal a los que no tenga autorización. En el **Anexo VI**, en el que se establece la relación de usuarios y perfiles de usuarios, se establecen también los accesos autorizados para cada uno de ellos, impidiéndose el acceso a datos que no requiera para el desempeño de sus funciones.

Exclusivamente el Responsable de Seguridad, o quien éste autorice por escrito, puede conceder, alterar o anular el acceso autorizado sobre los datos de carácter personal y recursos. Cuando el Responsable de Seguridad autorice a alguien para dichas funciones, se incluirá dicha autorización en el **Libro Registro de Autorizaciones** de la Empresa.

En caso de que exista personal ajeno al Responsable de los Ficheros que tenga acceso a los recursos, éste estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio de ***CHELO HISPANA, S.L..***

III. GESTIÓN DE SOPORTES Y DOCUMENTOS

Los soportes y documentos de ***CHELO HISPANA, S.L..*** que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen. Asimismo, serán inventariados y almacenados en un lugar con acceso restringido al personal autorizado en el presente Documento de Seguridad.

Cuando por las características físicas del soporte no sea posible el cumplimiento de las anteriores obligaciones, se dejará constancia motivada de ello a través de un Anexo específico al presente Documento de Seguridad.

En el **Anexo V** al presente Documento de Seguridad, se incluye el Inventario de soportes. Asimismo, en el **Anexo VI** se incluye la relación de usuarios con acceso autorizado a los lugares de custodia de los soportes.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del Responsable de los Ficheros deberá encontrarse debidamente autorizada en el presente Documento de Seguridad o bien ser autorizada por el Responsable de Seguridad, utilizando para ello el **Libro Registro de Salida de soportes** de quedispone la Empresa.

Asimismo, en el traslado de la documentación se adoptarán las medidas oportunas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte, utilizando para ello dispositivos de transporte con mecanismos que obstaculicen su apertura.

Cuando un soporte o documento vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el Inventario de soportes. Se incluye en el **Anexo VII** al presente Documento de Seguridad, el procedimiento de desecho o reutilización de soportes y documentos.

La identificación de los soportes que contengan datos de carácter personal considerados por parte de la Empresa como especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

IV. RÉGIMEN DE TRABAJO FUERA DE LAS OFICINAS

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del Responsable de los Ficheros, será preciso que exista una autorización previa y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

En relación con la necesaria autorización indicada en el párrafo anterior, se incluye en el **Anexo VIII** al presente Documento de Seguridad, una relación de las personas habilitadas por el Responsable de los Ficheros para otorgar dichas autorizaciones.

Asimismo, en el **Libro Registro de Autorizaciones** de la Empresa deberán constar las autorizaciones otorgadas, que podrán establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

También deberán constar en el **Libro Registro de Autorizaciones** las autorizaciones otorgadas a los Encargados del Tratamiento que, para la prestación del servicio contratado, requieran trabajar con los datos personales fuera de los locales del propio Encargado del Tratamiento.

V. NORMAS SOBRE EL USO DE ORDENADORES PORTÁTILES, PDA'S O MEMORY STICKS

Las normas contenidas en el presente Documento de Seguridad les serán plenamente aplicables a todas aquellas personas que precisen acceder y trabajar con datos de carácter personal a través de ordenadores portátiles o agendas electrónicas. Dichas personas serán, a todos los efectos, considerados usuarios del sistema.

El uso de ordenadores portátiles, PDA's o Memory Sticks con datos de carácter personal fuera de las instalaciones de la Empresa, deberá ser previamente autorizada, incluyéndose dicha autorización en el **Libro Registro de Autorizaciones.** La relación de las personas habilitadas por el Responsable de los Ficheros para otorgar dichas autorizaciones se incluye en el **Anexo IX** al presente Documento de Seguridad.

VI. FICHEROS TEMPORALES O COPIAS DE TRABAJO

Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares cumplirán el nivel de seguridad que les corresponda, atendiendo a la naturaleza de la información que contengan.

Todo fichero temporal o copia de trabajo será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Ficheros Temporales. Se deberá evitar el guardar copias de los datos personales del Fichero en archivos intermedios o temporales. En el caso de que sea imprescindible realizar esas copias temporales por exigencias del tratamiento, se deberán adoptar las siguientes precauciones:

- Realizar siempre esas copias sobre un mismo directorio de nombre TEMP o similar, de forma que no queden dispersas por todo el disco del ordenador y siempre se pueda conocer donde están los datos temporales.

- Tras realizar el tratamiento para los que han sido necesarios esos datos temporales, proceder al borrado o destrucción de los mismos.

Los ficheros temporales creados exclusivamente para la realización de trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de Medidas de Seguridad.

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del Fichero, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

El mantener un registro de las incidencias que comprometan la seguridad de un Fichero es una herramienta imprescindible para aplicar las medidas correctoras necesarias, así como posibilitar la prevención de posibles ataques a esa seguridad y la persecución de los responsables de los mismos.

MEDIDAS DE SEGURIDAD PARA FICHEROS NO AUTOMATIZADOS

*** Medidas de seguridad aplicables a los ficheros con datos de carácter personal no automatizados:**

1. A los ficheros no automatizados les será plenamente aplicable lo dispuesto en el presente Documento de Seguridad en cuanto a:

a) Control de accesos.
b) Gestión de soportes y documentos.
c) Régimen de trabajo fuera de los locales de la Empresa.
d) Copias de trabajo de documentos.
e) Funciones y obligaciones del personal.
f) Registro de incidencias.
g) Encargados del Tratamiento.

2. El archivo de los soportes o documentos se realizará con criterios que permitan la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. Se adjunta como Anexo X al presente Documento de Seguridad, el procedimiento de archivo y custodia de la documentación establecida por la Empresa.

3. Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.

4. Cuando, por sus características físicas, los dispositivos de almacenamiento utilizados no permitan adoptar la presente medida de seguridad, se adoptarán las medidas alternativas necesarias que impidan el acceso de personas no autorizadas. Dichas medidas alternativas se encuentran identificadas en el **Anexo IX** al presente Documento de Seguridad.

5. Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos al efecto, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

6. Deberá procederse a la destrucción de las copias o reproducciones desechadas que contengan datos de carácter personal, de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior. Para ello, se utilizará cualquier mecanismo de destrucción real y efectiva (por ejemplo, destructoras de papel).

ENCARGADO DEL TRATAMIENTO

Se entiende por Encargado del Tratamiento toda persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del Responsable de los Ficheros.

Como establece el párrafo 1 del artículo 9 de la LOPD, al hablar de la seguridad de los datos, "*el responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural*".

Atendiendo a lo dispuesto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, ***CHELO HISPANA, S.L..*** adoptará las medidas indicadas a continuación con el objetivo de cumplir con los requisitos legales previstos para los supuestos en que exista la figura del Encargado del Tratamiento.

1.- ***CHELO HISPANA, S.L.*** en calidad de Responsable de los Ficheros.

Cuando ***CHELO HISPANA, S.L.*** facilite el acceso a los datos, a los soportes que los contengan o a los recursos de los sistemas de información que los traten, a un Encargado de Tratamiento que preste sus servicios en los locales de la Empresa se reflejará tal circunstancia en el **Anexo X** del presente Documento de Seguridad, exigiendo al personal del Encargado el cumplimiento de las medidas de seguridad previstas en el presente Documento.

Cuando dicho acceso sea remoto, habiéndose prohibido al Encargado incorporar tales datos a sistemas o soportes distintos de los de ***CHELO HISPANA, S.L.*** se reflejará tal circunstancia en el mismo **Anexo X** del presente Documento de Seguridad, exigiendo al personal del Encargado el cumplimiento de las medidas de seguridad previstas en el presente Documento.

2.- ***CHELO HISPANA, S.L.*** en calidad de Encargado del Tratamiento.

En el momento en que ***CHELO HISPANA, S.L.*** preste a otras empresas determinados servicios que impliquen el acceso o tratamiento de datos de carácter personal, ostentará la condición de Encargado del Tratamiento respecto de los datos de aquéllas y deberá garantizar la seguridad de los datos de cuyo tratamiento se encargue.

En este sentido, ***CHELO HISPANA, S.L.*** deberá aplicar a los ficheros con datos de carácter personal de cuyo tratamiento se encargue en sus propios locales en calidad de Encargado del Tratamiento, las medidas de seguridad establecidas en el presente Documento de Seguridad, en función del nivel de seguridad que corresponda a los datos tratados.

La relación de dichos ficheros se detalla en el **Anexo II** al presente Documento de Seguridad, en el que se incluyen, además, la referencia expresa al contrato o documento que regula las condiciones del encargo, así como de la identificación del responsable, el nivel de las medidas de seguridad a implantar y el período de vigencia del encargo.

ESTRUCTURA DE LOS FICHEROS

En el **Anexo I** al presente Documento de Seguridad se detalla la estructura de los ficheros que contienen datos de carácter personal titularidad de ***CHELO HISPANA, S.L.***.

DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN

En los **Anexos III**, **IV** y **V** al presente Documento de Seguridad se describen los distintos recursos de los sistemas de información de ***CHELO HISPANA, S.L.*** en los que se almacenan o tratan los datos de carácter personal.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están claramente definidas y documentadas. El Responsable de los Ficheros adoptará las medidas necesarias para que el personal de ***CHELO HISPANA, S.L.*** conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento. Asimismo, establecerá las medidas necesarias para que periódicamente se revise el nivel de conocimiento de dichas funciones y obligaciones. En todo caso, en el momento en que una persona entre a trabajar en ***CHELO HISPANA, S.L.*** se le facilitará por escrito una copia de dichas funciones y obligaciones del personal y firmará en el cuadro adjunto que se incorpora.

Las funciones y obligaciones del personal en relación con el acceso a los sistemas de información de la Empresa y el tratamiento de los datos de carácter personal se detallan en el **Anexo XI** al presente Documento de Seguridad.

GESTIÓN Y REGISTRO DE INCIDENCIAS

En el **Anexo XII** al presente Documento de Seguridad, se define el procedimiento de notificación y gestión de las incidencias establecida por ***CHELO HISPANA, S.L.***.

Asimismo, para la gestión de dichas incidencias la Empresa dispone de un **Libro Registro de Incidencias** en el que se hace constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. En el mismo **Anexo XII** al presente Documento de Seguridad, se incorpora un modelo de hoja de dicho Registro de Incidencias.

COPIAS DE RESPALDO Y RECUPERACIÓN

En el **Anexo XIII** al presente Documento de Seguridad, se define el procedimiento de copias de respaldo y de recuperación establecido por la Empresa.

Dichos procedimientos establecidos por ***CHELO HISPANA, S.L.*** para la realización de copias de respaldo establecen una periodicidad mínima semanal, salvo que en dicho período no se haya producido ninguna actualización de los datos.

Asimismo, los procedimientos para la recuperación de los datos garantizarán en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos, quedando constancia motivada de este hecho en el presente Documento de Seguridad por medio del **Libro Registro de Incidencias**.

El Responsable de los Ficheros se encargará de verificar, como mínimo cada seis meses, la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el presente Documento de Seguridad mediante un Anexo específico. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente Documento de Seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en los sistemas de información, en los sistemas de tratamiento empleados, en la organización del mismo, en el contenido de la información incluida en los Ficheros o, en su caso, como consecuencia de los controles periódicos realizados. A estos efectos, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

En cualquier caso, como criterio de mínimos, se revisará el presente Documento de Seguridad una vez al año y se incluirán en el mismo las modificaciones que fueran necesarias.

Todas las revisiones y, en su caso, las modificaciones al presente Documento de Seguridad, observarán en todo momento la normativa vigente en materia de protección de datos de carácter personal.

CHELO HISPANA, S.L.

ANEXOS DOCUMENTO DE SEGURIDAD

ANEXOS

I. IDENTIFICACIÓN Y ESTRUCTURA DE LOS FICHEROS TITULARIDAD DE LA EMPRESA

II. IDENTIFICACIÓN DE LOS FICHEROS TRATADOS POR LA EMPRESA EN CALIDAD DE ENCARGADO DEL TRATAMIENTO

III. EQUIPOS QUE TRATAN O ALMACENAN DATOS DE CARÁCTER PERSONAL

IV. PROGRAMAS O APLICACIONES INFORMÁTICAS

V. SOPORTES INFORMÁTICOS

VI. USUARIOS AUTORIZADOS

VII. PROCEDIMIENTOS DE IDENTIFICACIÓN Y AUTENTICACIÓN

VIII. PERSONAS HABILITADAS PARA OTORGAR AUTORIZACIONES

IX. PROCEDIMIENTO DE ARCHIVO DE LA DOCUMENTACIÓN

X. ENCARGADOS DEL TRATAMIENTO DE FICHEROS TITULARIDAD DE LA EMPRESA

XI. FUNCIONES Y OBLIGACIONES DEL PERSONAL

XII. PROCEDIMIENTO DE NOTIFICACIÓN Y GESTIÓN DE INCIDENCIAS

XIII. PROCEDIMIENTO DE COPIAS DE RESPALDO Y DE RECUPERACIÓN

ANEXO I

IDENTIFICACIÓN Y ESTRUCTURA DE LOS FICHEROS CON DATOS DE CARÁCTER PERSONAL TITULARIDAD DE LA EMPRESA

A) Fichero de PROVEEDORES:

i Código de inscripción del fichero:

ii Descripción del contenido del fichero: GESTION DE PROVEEDORES

iii Nivel de seguridad: BASICO

iv Estructura del fichero: NOMBRE Y APELLIDOS, DIRECCIÓN, DNI, TELÉFONO, E-MAIL, DATOS BANCARIOS, CUALQUIER DATO NECESARIO PARA LLEVAR A CABO LA RELACIÓN COMERCIAL

v Información general:

- Encargado del Tratamiento: ; GESTIÓN LUCENA S.L. C/ San Pedro, 40 Lucena 14900 (Córdoba)
- Finalidad y usos previstos: GESTION DE PROVEEDORES CONTABLE, FISCAL Y ADMINISTRATIVA, CONTROL DE PAGOS
- Cesiones previstas: ORGANISMOS DE LA ADMINISTRACIÓN PÚBLICA CON COMPETENCIA EN LA MATERIA, CUALQUIER ORGANISMO RELACIONADO CON EL RESPONSABLE DE LOS FICHEROS, BANCOS Y CAJAS DE AHORRO.
- Transferencias internacionales: NO SE HAN PREVISTO
- Procedencia de los datos: PROPIO INTERESADO O REPRESENTANTE
- Procedimiento de recogida: EN VIRTUD DE RELACION COMERCIAL
- Soporte empleado para la recogida de datos: SOPORTE PAPEL Y AUTOMATIZADO
- Centro donde se tratan los datos: C/ SIERRA DE ARAS, 9 LUCENA (CORDOBA) 14900;

vi Servicio ante el que ejercitar los derechos de acceso, rectificación, cancelación y oposición: CHELO HISPANA, S.L., C/ SIERRA DE ARAS, 9 14900 LUCENA (CORDOBA)

B) Fichero de CLIENTES:

i Código de inscripción del fichero:

ii Descripción del contenido del fichero: GESTION DE CLIENTES CONTABLE FISCAL Y ADMINISTRATIVA.

iii Nivel de seguridad: BÁSICO

iv Estructura del fichero: NOMBRE Y APELLIDOS, DNI, DIRECCIÓN, TELÉFONO, DATOS BANCARIOS, CUALQUIER DATO NECESARIO PARA EL DESARROLLO DE LA PRESTACIÓN DE SERVICIOS POR LA EMPRESA

v Información general:

- Encargado del Tratamiento: ; GESTIÓN LUCENA S.L. C/ San Pedro, 40 Lucena 14900 (Córdoba)
- Finalidad y usos previstos: GESTIÓN DE CLIENTES CONTABLE, FISCAL Y ADMINISTRATIVA
- Cesiones previstas: ORGANISMOS DE LA ADMINISTRACIÓN PÚBLICA CON COMPETENCIA EN LA MATERIA, ORGANISMOS RELACIONADOS CON EL RESPONSABLE DE LOS FICHEROS, BANCOS Y CAJAS DE AHORRO, JUZGADOS Y TRIBUNALES
- Transferencias internacionales: NO SE HAN PREVISTO
- Procedencia de los datos: PROPIO INTERESADO O REPRESENTANTE
- Procedimiento de recogida: EN VIRTUD DE RELACION COMERCIAL
- Soporte empleado para la recogida de datos: SOPORTE PAPEL Y AUTOMATIZADO
- Centro donde se tratan los datos: C/ SIERRA DE ARAS, 9 LUCENA (CORDOBA) 14900;

vi Servicio ante el que ejercitar los derechos de acceso, rectificación, cancelación y oposición: CHELO HISPANA, S.L., C/ SIERRA DE ARAS, 9 14900 LUCENA (CORDOBA)

C) Fichero de CORREO ELECTRONICO:

i Código de inscripción del fichero:

ii Descripción del contenido del fichero: APLICACION PARA LA GESTION DEL CORREO ELECTRONICO, ASI COMO LA AGENDA DE CONTACTOS

iii Nivel de seguridad: BÁSICO

iv Estructura del fichero: NIF/DNI, NOMBRE Y APELLIDOS, DIRECCION, TELEFONO, FIRMA/HUELLA, ECONOMICOS, FINANCIEROS Y DE SEGUROS, TRANSACCIONES DE BIENES Y SERVICIOS, DIRECCION ELECTRONICA

v Información general:

- Encargado del Tratamiento:
- Finalidad y usos previstos: GESTIÓN DE CLIENTES CONTABLE, FISCAL Y ADMINISTRATIVA, GUIAS/REPERTORIOS DE SERVICIOS DE COMUNICACIONES ELECTRONICAS
- Cesiones previstas: NO SE HAN PREVISTO
- Transferencias internacionales: NO SE HAN PREVISTO
- Procedencia de los datos: EL PROPIO INTERESADO O SU REPRESENTANTE LEGAL
- Procedimiento de recogida: EN VIRTUD DE LA RELACION MUTUA
- Soporte empleado para la recogida de datos: SOPORTE AUTOMATIZADO
- Centro donde se tratan los datos: C/ SIERRA DE ARAS, 9 LUCENA (CORDOBA) 14900;

vi Servicio ante el que ejercitar los derechos de acceso, rectificación, cancelación y oposición: CHELO HISPANA, S.L., C/ SIERRA DE ARAS, 9 14900 LUCENA (CORDOBA)

ANEXO II

IDENTIFICACIÓN DE LOS FICHEROS TRATADOS POR LA EMPRESA EN CALIDAD DE ENCARGADO

CHELO HISPANA, S.L. puede realizar el tratamiento de distintos ficheros con datos de carácter personal en calidad de Encargado del Tratamiento, según lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La relación de los ficheros tratados por parte de ***CHELO HISPANA, S.L.*** en calidad de Encargado del Tratamiento y cuyo tratamiento se realiza en los propios locales de la Empresa se encuentran identificados en el archivo **ENCARGOS DE TRATAMIENTOS**, ajunto al presente documento de seguridad.

En dicho archivo se incluye, además, la referencia expresa al contrato o documento que regula las condiciones del encargo, así como la identificación del responsable, el nivel de las medidas de seguridad a implantar y el período de vigencia del encargo.

Las empresas que prestan servicios sin acceso a datos al responsable del fichero son las relacionadas en el archivo **EMPRESAS PRESTADORAS DE SERVICIOS**, ajunto al presente documento de seguridad.

ANEXO III

EQUIPOS QUE TRATAN O ALMACENAN DATOS DE CARÁCTER PERSONAL

La relación actualizada de los equipos mediante los cuales se tratan, transmiten o almacenan datos de carácter personal en ***CHELO HISPANA, S.L.*** se encuentra referenciada al archivo denominado **EQUIPOS**, ajunto al presente documento de seguridad.

En dicho archivo se especifican las características técnicas de los equipos de tratamiento y almacenamiento de datos personales utilizados por ***CHELO HISPANA, S.L.***.

ANEXO IV

PROGRAMAS O APLICACIONES INFORMÁTICAS

La relación actualizada de los programas o aplicaciones informáticas utilizados por ***CHELO HISPANA, S.L.*** para el tratamiento o almacenamiento de datos de carácter personal se encuentra referenciada al archivo denominado **FUNCIONES Y OBLIGACIONES DEL PERSONAL**, ubicado en el directorio "LOPD" del Servidor.

ANEXO V

SOPORTES INFORMÁTICOS

---

1. ***Procedimiento de inventario, identificación y custodia***

Los soportes utilizados por ***CHELO HISPANA, S.L.*** se identifican y custodian mediante el sistema descrito a continuación.

a) Inventario:

El Responsable de Seguridad lleva una relación detallada de los soportes que contienen datos de carácter personal.

La relación completa y actualizada de los soportes informáticos utilizados por ***CHELO HISPANA, S.L.*** se encuentra referenciada al archivo **FUNCIONES Y OBLIGACIONES DEL PERSONAL**, ubicado en el directorio "LOPD" del Servidor.

b) Identificación:

Cada uno de los soportes que contienen datos de carácter personal deberá estar debidamente etiquetado y su identificador coincidirá con el del Inventario de soportes.

Cuando las características físicas del soporte imposibiliten su etiquetado, quedará constancia motivada de ello en el propio Inventario de soportes.

La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles y de aquellos que contengan datos de nivel alto, se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

c) Almacenamiento o custodia:

Los soportes que contengan datos de carácter personal serán almacenados en un lugar con acceso restringido, accesibles únicamente al personal autorizado según la relación de usuarios del **Anexo VI** del presente Documento de Seguridad.

2. ***Procedimiento de desecho o reutilización***

Cuando un soporte vaya a ser desechado o reutilizado se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él. A estos efectos, antes de reutilizar cualquier soporte, se procederá al formateo del mismo.

Asimismo, para la destrucción de soportes que contengan datos de carácter personal, se deberán aplicar las medidas de desmagnetización o destrucción física que aseguren la imposibilidad de recuperar la información del soporte.

Una vez finalizado el proceso, se procederá a dar de baja los soportes destruidos en el Inventario.

Procedimiento para la destrucción de desechos informáticos.

Todos los desechos informáticos de cualquier tipo que puedan contener información del Fichero, como CDs, cintas, discos removibles, listados, memorias removibles de cualquier tipo, o incluso los propios ordenadores obsoletos que contengan discos e almacenamiento, deberán ser eliminados o destruidos de acuerdo con el siguiente Procedimiento para la Destrucción de Desechos Informáticos.

1. Como norma general ningún desecho informático, ya sea listado u otro tipo de soporte, debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.

2. Aquellos informes en papel o CDs que contengan datos de carácter personal más sensible y no sean voluminosos, deberán ser destruidos en una destructora de papel si es que existe en la organización.

3. En caso de no existir máquina destructora de papel y CDs o en le caso de que los listados e informes sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una compañía de reciclaje que garantice mediante contrato la destrucción de los mismos.

4. Todos los disquetes y otros soportes removibles desechados deberán ser formateados y entregados para su reutilización al Responsable de Seguridad o al Responsable del Fichero. En el caso de que no se vayan a reutilizar deberán ser formateados si se puede, y depositados en los Contenedores confidenciales de la organización para ser entregadas a la empresa encarga da de la destrucción de los datos.

5. Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras instituciones, deberá comunicarse al Responsable de Seguridad para que se formatee el disco duro o se pase un programa especial que elimine de forma segura todos los datos de los discos duros. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y depositarlos en le Contenedor de la empresa de reciclaje para su destrucción.

6. El responsable del fichero deberá exigir a la empresa de reciclaje un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

ANEXO VI

USUARIOS AUTORIZADOS

---

1. ***Usuarios con acceso autorizado a los sistemas de información***

La relación actualizada de los usuarios que tienen acceso a los sistemas de información y a los datos de carácter personal se encuentra referenciada al archivo **FUNCIONES Y OBLIGACIONES DEL PERSONAL**, ubicado en el directorio “LOPD” del Servidor.

2. ***Usuarios con acceso autorizado a los soportes***

La relación actualizada del personal autorizado a acceder al lugar en el que se almacenan los soportes de la Empresa se encuentra referenciada al mismo archivo **FUNCIONES Y OBLIGACIONES DEL PERSONAL** ubicado en el directorio “LOPD” del Servidor.

3. ***Usuarios con acceso autorizado a los lugares donde se encuentran los equipos que dan soporte a los sistemas de información que tratan o almacenan datos de nivel medio***

La relación actualizada del personal autorizado a acceder a los lugares donde se hallan instalados los equipos que dan soporte a los sistemas de información que tratan datos de nivel medio y/o alto se encuentra referenciada al archivo **FUNCIONES Y OBLIGACIONES DEL PERSONAL** ubicado en el directorio “LOPD” del Servidor.

ANEXO VII

PROCEDIMIENTOS DE IDENTIFICACIÓN Y AUTENTICACIÓN

En el presente Anexo se describen de forma detallada los mecanismos establecidos por ***CHELO HISPANA, S.L.*** para la gestión de los usuarios de los sistemas de información de la Empresa, junto con los procedimientos y medidas desarrollados para garantizar los aspectos recogidos en el Reglamento de Protección de Datos (R.D. 1720/2007).

Los mecanismos de identificación y autenticación en los sistemas y aplicaciones de ***CHELO HISPANA, S.L.*** se basan en el uso de cuentas de usuario, que se componen de un código de usuario o identificador y contraseña o clave de acceso.

1. ***Gestión de usuarios***

Las solicitudes de acceso sobre los sistemas de información deberán enviarse por medio de correo electrónico y deberán ser aprobadas por el Responsable del Área a la que pertenezcan los usuarios que requieran el acceso.

Dichas peticiones, debidamente cumplimentadas, serán analizadas por el Responsable de Seguridad.

En caso de autorización, el Responsable de Seguridad o en quien éste delegue, realizará la operación solicitada. En caso contrario, se informará al peticionario indicando el motivo del rechazo.

Para las bajas, modificaciones y petición de cambios en los perfiles de usuario se procederá de idéntica forma.

2. ***Identificación y autenticación***

La parametrización de los mecanismos de identificación y autenticación de ***CHELO HISPANA, S.L.*** deberá cumplir con los siguientes requisitos de seguridad:

- Los identificadores de usuario se construirán, con carácter general, de acuerdo a la inicial del nombre y el primer apellido.

- La contraseña asignada por defecto será generada de manera aleatoria para cada usuario.

- Las contraseñas deberán constar de un mínimo de 6 caracteres alfanuméricos, aleatoriamente seleccionados en orden y número, no pudiendo incluir caracteres del tipo comas, puntos, paréntesis, barras, contrabarras o caracteres de puntuación en general, signos de admiración, de interrogación o similares. Es recomendable que dos de los caracteres que conformen la contraseña sean números del 0 al 9, ambos incluidos.

- Siempre que el sistema o la aplicación lo contemplen técnicamente, se permitirá al usuario cambiar su contraseña.
- Siempre que el sistema o la aplicación lo contemplen técnicamente, se forzará el cambio de contraseña en el primer login al sistema.
- Se forzará el cambio periódico de contraseña, como mínimo, cada 12 meses. En ningún caso podrán repetirse contraseñas que hayan sido válidas y con efecto durante las dos últimas asignaciones.
- Podrán asignarse nuevas contraseñas con anterioridad a la expiración del plazo indicado, cuando alguna incidencia ocurrida en el sistema así lo aconseje, o cuando algún usuario lo solicite por haber perdido su contraseña vigente.
- Para los entornos y aplicaciones informáticas que manejen datos de carácter personal de nivel medio y/o alto, se limitará el número de intentos de acceso fallidos a cinco, con desbloqueo manual de los usuarios por parte de un administrador autorizado.
- Se prohíbe la existencia de usuarios genéricos con acceso a datos de carácter personal.

3. ***Procedimiento de asignación y distribución de contraseñas***

El Responsable de Seguridad y, por delegación de éste, los administradores de los entornos informáticos existentes en la Empresa serán los únicos autorizados para definir, asignar y revocar las contraseñas asociadas a los usuarios de los sistemas y aplicaciones, de acuerdo a los siguientes criterios:

- La contraseña se creará de manera individual y aleatoria para cada usuario.
- Se evitará el uso de contraseñas iniciales comunes o por defecto, así como la asignación de contraseñas iniciales fácilmente transferibles (contraseñas coincidentes con el identificador de usuario, con el nombre o DNI del mismo...).

El usuario y contraseña serán entregados a los usuarios por correo electrónico o mediante comunicación directa del administrador al empleado.

4. ***Procedimiento de almacenamiento de contraseñas***

Las contraseñas se almacenarán en lugar seguro dentro de los propios sistemas informáticos y de forma ininteligible.

Las contraseñas de acceso a los sistemas de información son personales e intransferibles, por lo que cada usuario deberá garantizar la absoluta confidencialidad de su contraseña. En este sentido, ante cualquier incidencia relativa al conocimiento de la contraseña por parte de terceras personas, deberá comunicarse inmediatamente al Responsable de Seguridad, procediéndose a su modificación.

ANEXO VIII

PERSONAS HABILITADAS PARA OTORGAR AUTORIZACIONES

La relación de las personas habilitadas por el Responsable de los Ficheros para otorgar las autorizaciones previstas en el presente Documento de Seguridad es la que se indica a continuación.

Asimismo, a los efectos de dejar constancia escrita de las autorizaciones emitidas por las personas habilitadas en el presente Anexo, la Empresa dispone de un **Libro Registro de Autorizaciones**. En el **Registro de Incidencias** y en los **Registro de Entrada y Salida de Soportes** también se anotan algunas de las autorizaciones previstas.

PERSONAS HABILITADAS PARA OTORGAR AUTORIZACIONES:

1. Autorización para almacenar datos en dispositivos portátiles o para tratar datos fuera de los locales del Responsable de los Ficheros.

Persona habilitada:
Lugar de registro de las autorizaciones: Libro Registro de Autorizaciones.

2. Autorización dirigida a los Encargados del Tratamiento que, para la prestación del servicio contratado, requieran trabajar con los datos personales fuera de los locales del propio encargado del tratamiento.

Persona habilitada:
Lugar de registro de las autorizaciones: Libro Registro de Autorizaciones.

3. Autorización de personas responsables de la recepción de soportes y documentos con datos de nivel medio o alto.

Persona habilitada:
Lugar de registro de las autorizaciones: Registro de Entrada de Soportes.

4. Autorización de personas responsables de la entrega de soportes y documentos con datos de nivel medio o alto.

Persona habilitada:
Lugar de registro de las autorizaciones: Registro de Entrada de Soportes.

5. Autorización para ejecutar procedimiento de recuperación de datos.

Persona habilitada:
Lugar de registro de las autorizaciones: Registro de Incidencias.

ANEXO IX

PROCEDIMIENTO DE ARCHIVO DE LA DOCUMENTACIÓN

Los mecanismos establecidos por ***CHELO HISPANA, S.L.*** para la custodia y archivo de la documentación en papel se describen a continuación y son de obligado cumplimiento para todo el personal.

1. Organización física de los archivos

Todos los documentos deberán ir clasificados en expedientes o carpetas que estarán debidamente marcadas en base al Área o Departamento que las genera, así como con la fecha y la temática o proyecto cuya información contengan.

Ejemplo genérico:

ÁREA (Depto.):	Nombre del Departamento de origen.
TEMA:	Se indicará el asunto general de la documentación.
FECHA:	Se anotarán las fechas extremas de la documentación.

Ejemplo Concreto

ÁREA (Depto.):	Recursos Humanos.
TEMA:	Nóminas
FECHA:	Enero - Diciembre 2008

ÁREA (Depto.):	Dpto. Técnico
TEMA:	Cliente A
FECHA:	Junio - Julio 2008

La organización al interior de las carpetas deberá ser de forma cronológica ascendente.

Si un asunto o tema genera muchos documentos, deberán abrirse más carpetas con la misma identificación. Esto evitará el deterioro físico y la incomodidad para consultarlo.

2. Dispositivos de almacenamiento

Los documentos o carpetas que contengan datos de carácter personal deberán almacenarse obligatoriamente en archivadores, armarios o cajones cerrados bajo llave. Dichos dispositivos de almacenamiento no deberán en ningún caso conservar la llave puesta en la cerradura.

Asimismo, cuando la documentación contenga datos de carácter personal de nivel alto, los armarios, archivadores u otros elementos en los que se almacenen dichos documentos deberán encontrarse en áreas o despachos en los que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas o despachos deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

Si, atendidas las características de los locales de la Empresa, en algún momento no fuera posible cumplir con lo establecido en el párrafo anterior, la Empresa garantizará la presencia constante en horario de trabajo de una persona autorizada que custodiará la documentación. Fuera del horario propio de oficinas, la documentación quedará protegida mediante las puertas de acceso principales a las oficinas o instalaciones de la Empresa.

3. Custodia de los archivos

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos al efecto por la Empresa, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada. Para ello, se deberán guardar los documentos que contengan datos personales protegidos en un sitio que no pueda ser visible para terceros.

ANEXO X

ENCARGADOS DEL TRATAMIENTO DE FICHEROS TITULARIDAD DE LA EMPRESA

La relación de Encargados del Tratamiento que prestan servicios en los locales de ***CHELO HISPANA, S.L.*** y que acceden a los datos, a los soportes que los contienen o a los recursos de los sistemas de información que los tratan se encuentra referenciada al archivo **ENCARGADOS DEL TRATAMIENTO**, adjunto al presente documento de seguridad.

Asimismo, en el mismo archivo **ENCARGADOS DEL TRATAMIENTO** se incluye la relación de Encargados con acceso remoto a los datos o a los recursos de los sistemas de información de ***CHELO HISPANA, S.L.*** y a los que se ha prohibido incorporar tales datos a sistemas o soportes distintos de los de ***CHELO HISPANA, S.L.***.

El personal de los Encargados del Tratamiento deberá cumplir con las medidas de seguridad previstas en el presente Documento de ***CHELO HISPANA, S.L.***, por lo que la Empresa facilitará a los trabajadores de los Encargados una copia del documento Funciones y Obligaciones del Personal de ***CHELO HISPANA, S.L.***.

ANEXO XI

FUNCIONES Y OBLIGACIONES DEL PERSONAL

Las funciones y obligaciones de cada una de las personas que forman parte de ***CHELO HISPANA, S.L.*** y que tienen acceso a los datos de carácter personal y a los sistemas de información son las que se relacionan a continuación.

En caso de incumplimiento de las presentes funciones y obligaciones por parte de cualquier trabajador de ***CHELO HISPANA, S.L.***, la Dirección de la Empresa, de conformidad con la legislación vigente, podrá adoptar las sanciones que tenga estipuladas, así como reclamar las responsabilidades civiles y penales que legalmente correspondan.

1. ***PERSONAL DE NOMBRE DE LA EMPRESA***

Datos de carácter personal

a) El personal de ***CHELO HISPANA, S.L.*** únicamente tiene acceso autorizado a los datos de carácter personal y a los sistemas de información cuando lo precisen para el desarrollo de sus funciones.

b) Las personas con acceso autorizado a los ficheros de ***CHELO HISPANA, S.L.*** a través de su puesto de trabajo no podrán modificar la configuración de las aplicaciones ni del sistema operativo, salvo autorización expresa de la Empresa.

c) El personal de ***CHELO HISPANA, S.L.*** única y exclusivamente podrá utilizar aquellos datos de carácter personal a los que tenga acceso en virtud de sus funciones para dar cumplimiento a sus obligaciones laborales, quedando expresa y completamente prohibida cualquier otra utilización.

d) El personal de ***CHELO HISPANA, S.L.*** no podrá borrar, destruir, dañar, alterar o modificar cualquiera de los datos de carácter personal que contengan las bases de datos de ***CHELO HISPANA, S.L.*** sin la autorización expresa de la Empresa, siempre y cuando no sea en ejercicio de las funciones que le han sido encomendadas.

e) Cada trabajador de ***CHELO HISPANA, S.L.*** que, por razón del ejercicio de sus funciones, tenga acceso a los datos deberá observar la debida reserva, confidencialidad y sigilo en relación con los mismos. Esta obligación perdurará incluso tras finalizar su vinculación con la Empresa.

f) El personal de ***CHELO HISPANA, S.L.*** no podrá realizar copias, transmisiones, comunicaciones o cesiones de los datos de carácter personal tratados por ***CHELO HISPANA, S.L.*** sin la autorización expresa de la Empresa, siempre y cuando no sea en ejercicio de las funciones que le han sido encomendadas.

g) El personal de ***CHELO HISPANA, S.L.*** tendrá la obligación de comunicar cualquier incidencia, anomalía, error o fallo que detectara en los ficheros o sistemas de información propiedad de***CHELO HISPANA, S.L.***.

h) El uso de ordenadores portátiles, PDA's o Memory Sticks con datos de carácter personal fuera de las instalaciones de la Empresa deberá comunicarse previamente al Responsable de Seguridad, quien deberá otorgar la correspondiente autorización.

i) Todo fichero temporal o copia de trabajo será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

j) Está estrictamente prohibido copiar información de carácter personal incluida en los ficheros de ***CHELO HISPANA, S.L.*** en cualquier tipo de soporte informático (Disquette, DVD, Memory Sticks, etc.) sin la autorización previa y expresa de la Empresa. En caso de haber sido autorizada la utilización de cualquier soporte informático, el usuario deberá comunicarlo inmediatamente al Responsable de Seguridad para su inventario y etiquetado.

k) Cualquier salida de soportes informáticos que contengan datos de carácter personal (Disquette, DVD, Memory Sticks, etc.) fuera de las instalaciones de ***CHELO HISPANA, S.L.*** deberá ser autorizada de forma previa y expresa por parte de la Empresa.

l) En el supuesto de recibir cualquier soporte informático que contenga datos de carácter personal procedente del exterior de la Empresa, el usuario deberá comunicarlo al Responsable de Seguridad a los efectos de poder anotarlo en el Registro de Entrada de Soportes.

m) Cuando un soporte deba ser desechado, se deberá entregar al Responsable de Seguridad para que pueda proceder a su destrucción y baja en el Inventario de Soportes.

n) El personal de ***CHELO HISPANA, S.L.*** deberá comunicar a los Responsables de Área cualquier solicitud de acceso, rectificación, cancelación u oposición de datos de carácter personal presentada por parte de algún afectado. Dicha comunicación deberá realizarse en el plazo máximo de 3 horas desde la recepción de la solicitud.

Claves de acceso o identificadores de usuario

a) Cada trabajador de ***CHELO HISPANA, S.L.*** que en el desarrollo de sus funciones laborales realice actividades en las cuales sea necesario acceder a los ficheros de datos de carácter personal propiedad de ***CHELO HISPANA, S.L.***, dispondrá de un nombre de usuario que le identifique única y exclusivamente a él y de una clave o contraseña personal que le permita, durante el proceso de acceso a los datos, autenticarse como usuario autorizado.

b) Dicho nombre de usuario o identificador así como la correspondiente contraseña, será personal e intransferible. Queda absolutamente prohibida su revelación a cualquier otra persona sin la autorización expresa de la Empresa.

c) En los supuestos en los que la aplicación informática lo permita, el usuario deberá modificar su contraseña de acceso la primera vez que acceda a la aplicación.

d) La contraseña de acceso o password deberá cambiarse de manera obligatoria, como mínimo anualmente, aún en el caso de que la aplicación no obligue a ello. Esto es aplicable a todas las aplicaciones informáticas utilizadas en la Empresa, así como a todos aquellos recursos informáticos que requieran identificación previa y permitan el cambio de la clave de acceso.

e) Cada trabajador será responsable de conservar de forma confidencial y segura su nombre de usuario (identificador único) y su contraseña personal. En los supuestos que el trabajador tuviera la certeza o sospechara que alguien está utilizando dichos identificadores o contraseñas, podrá solicitar a la Empresa que le asigne un identificador y contraseña nuevos.

f) Dicho identificador único y la contraseña sólo podrán utilizarse dentro de los locales de ***CHELO HISPANA, S.L.*** Queda expresamente prohibido el acceso desde fuera de los locales de ***CHELO HISPANA, S.L.*** sin la autorización expresa de la Empresa.

g) Cada trabajador deberá evitar que los datos contenidos en los ficheros sean visibles a través de sus puestos de trabajo por personas no autorizadas. Para ello, cuando un trabajador abandone su puesto de trabajo (para el desayuno, reuniones, comida, etc.) deberá apagar el equipo o utilizar un protector de pantalla con la contraseña correspondiente.

Sistemas de comunicación

a) En caso de tener que enviar correos electrónicos a más de un destinatario a la vez, es obligatorio utilizar la opción de copia oculta (CCO). En caso de duda sobre dicha funcionalidad, puede consultarse con cualquier Responsable de Área.

b) El personal de ***CHELO HISPANA, S.L.*** no podrá utilizar sistemas de comunicación para transmitir datos de carácter personal si éstos no han sido expresamente autorizados por parte del Responsable de Fichero.

Tratamiento de los datos en servidor

a) Todos los datos de carácter personal que sean objeto de tratamiento por parte de los trabajadores, deberán ubicarse y/o tratarse en los servidores de la Empresa. El personal de ***CHELO HISPANA, S.L.*** no podrá alojar ningún tipo de dato de carácter personal en el disco duro de sus ordenadores personales.

Tratamiento de documentación en papel

a) Los documentos que contengan datos de carácter personal deberán almacenarse siempre en los armarios y archivadores establecidos al efecto y que dispongan de los oportunos mecanismos de cierre que obstaculicen su apertura.

b) Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento previstos por la Empresa, por estar en proceso de revisión o tramitación, el trabajador que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada. Para ello, se deberán guardar los documentos que contengan datos personales protegidos en un sitio que no pueda ser visible para terceros.

c) Cada trabajador será responsable de proceder a la destrucción de las copias o reproducciones desechadas, de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior. Se recomienda la utilización de destructoras de papel.

d) Siempre que se proceda al traslado físico de la documentación contenida en un fichero, se deberán adoptar medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

e) En el uso de impresoras, faxes y fotocopiadoras se debe retirar la documentación relativa a los datos personales inmediatamente después de su impresión, envío o copia evitando el acceso por parte de personas no autorizadas.

2. ***PERSONAL DE ENCARGADOS DEL TRATAMIENTO***

El personal de cualquier Encargado del Tratamiento contratado por ***CHELO HISPANA, S.L.*** que preste servicios en las oficinas o instalaciones de la Empresa o que acceda a los ficheros de ***CHELO HISPANA, S.L.*** de forma remota, deberá cumplir con las mismas medidas de seguridad previstas en el apartado anterior para el personal en plantilla.

ANEXO XII

PROCEDIMIENTO DE NOTIFICACIÓN Y GESTIÓN DE INCIDENCIAS

El objeto del presente procedimiento es establecer y describir un procedimiento de notificación y gestión de incidencias, tal y como exige el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

El presente procedimiento es aplicable a todas las personas vinculadas con ***CHELO HISPANA, S.L.*** y que traten datos de carácter personal incluidos en ficheros que sean responsabilidad de la Empresa.

Se incluye a continuación un listado de los eventos más comunes que deberían ser considerados como incidencias de seguridad, y por lo tanto, reportados a través de los canales de gestión de incidencias establecidos. Sin embargo, dicho listado no pretende ser una enumeración exhaustiva de las mismas.

- Pérdida, robo o extravío de equipos portátiles.
- Pérdida, robo o extravío de documentación en papel.
- Pérdida, robo o extravío de soportes informáticos.
- Contraseñas de acceso al sistema que hayan visto comprometida su confidencialidad.
- Fallos en los procesos de copias de seguridad o de restauración de datos.
- Comportamientos anómalos/errores de sistemas, aplicaciones y bases de datos que manejen datos de carácter personal y que puedan afectar a la seguridad de la información.
- Accesos no autorizados a los sistemas de información de la Empresa.
- Accesos físicos no autorizados a las instalaciones de la Empresa, especialmente a la sala de servidores o CPD.
- Desaparición o alteración de ficheros informáticos.

El proceso de gestión de incidencias llevará asociado una serie de actividades que se detallan en los siguientes apartados. Estas actividades se agruparán en las siguientes fases:

a) Detección de incidencia.
b) Comunicación de la incidencia.
c) Resolución de incidencias.
d) Cierre de incidencia.
e) Registro de la incidencia.

a) Detección de la incidencia

Una incidencia puede ser detectada en cualquiera de las fases del tratamiento de los datos de carácter personal incluidos en los ficheros que sean responsabilidad de ***CHELO HISPANA, S. L.***, ya sea en calidad de Responsable o de Encargado del Tratamiento.

Una vez detectada, la persona que detectó la incidencia deberá notificarlo al Responsable de Seguridad, o en quien éste delegue, para que proceda a su registro.

b) Comunicación de la incidencia

Los usuarios emplearán cualquier canal de comunicación de las incidencias que se produzcan en su entorno de trabajo. La comunicación deberá producirse tan pronto como se detecte la misma. En dicha comunicación se deberá incluir, al menos, la siguiente información:

- Descripción de la incidencia.
- Efectos que se han derivado de la misma.
- Entorno informático e información afectada.
- Persona que ha detectado la incidencia (sí es distinta del comunicante).
- Fecha y hora en la que ha ocurrido la incidencia o se ha tenido conocimiento de la misma.

c) Resolución de la incidencia

Cuando de la resolución de la incidencia pueda derivarse una pérdida de integridad, confidencialidad o disponibilidad, se deberá pedir autorización al Responsable de Seguridad, para realizar cualquier operación.

Excepcionalmente podrá prescindirse de autorización previa cuando concurran circunstancias de fuerza mayor o ante posibilidad cierta de degradación del servicio que se presta sobre la base del fichero.

d) Cierre de la incidencia

El cierre de una incidencia es responsabilidad del Responsable de Seguridad.

El cierre de la incidencia deberá ser informado a toda aquella persona implicada en cualquiera de las fases de su detección y resolución. Se informará del cierre de la incidencia por los mismos canales previstos para su comunicación.

Se considerará cerrada cuando toda persona implicada en cualquiera de las anteriores fases esté conforme con la solución, quedando fechada y visada en el Registro de Incidencias.

e) Registro de la incidencia

El Responsable de Seguridad deberá asegurarse de que las incidencias quedan debidamente anotadas en el Registro de Incidencias de la Empresa. De todas las incidencias acaecidas en la Empresa se mantendrá un histórico durante, al menos, los dos últimos años.

El Registro de Incidencias de ***CHELO HISPANA, S.L.*** constará en documento aparte y deberá contener los campos que figuren en la siguiente ficha.

HOJA DE INCIDENCIA					
Nº de Incidencia:	[nº/año]	**Fecha:**	[dd/mm/aaaa]	**Hora:**	[hh:mm]
Persona que Notifica la Incidencia:					
Persona a quien se Notifica la Incidencia:					
Tipo de incidencia:					
Efectos:					
Medidas Correctoras aplicadas:					
Procedimientos de recuperación de datos:					
Persona que realiza la restauración:					
Datos restaurados:					
Datos restaurados o grabados manualmente:					
Responsable del fichero:			**Firma:**		

ANEXO XIII

PROCEDIMIENTO DE COPIAS DE RESPALDO Y DE RECUPERACIÓN

En el presente procedimiento se describen de forma detallada los mecanismos establecidos por ***CHELO HISPANA, S.L.*** para la realización de copias de respaldo sobre los datos residentes en sus sistemas de información y para la recuperación de los mismos, junto con los procedimientos y medidas desarrollados para garantizar los aspectos recogidos al respecto en el Reglamento de Protección de Datos (R.D. 1720/2007).

El Responsable de Seguridad es la persona encargada de comprobar la operatividad y correcto funcionamiento de los procedimientos de realización de copias de seguridad y de recuperación de datos al menos semestralmente.

1. ***Procedimiento de copias de respaldo***

Los procedimientos aquí descritos se aplican sobre todos los servidores y sistemas utilizados por ***CHELO HISPANA, S.L.*** y que almacenan datos de carácter personal.

Se harán copias de respaldo completas de los servidores de producción con una periodicidad mínima semanal. Este backup semanal se establece como criterio de mínimos.

En cualquier caso, la Empresa intentará dotarse de los recursos necesarios que le permitan disponer de una copia de respaldo con periodicidad diaria (de lunes a viernes). En estos casos, la copia de seguridad correspondiente al último día de la semana se conservará a modo de backup semanal.

Antes de guardar los soportes que contengan las copias semanales en los dispositivos de almacenamiento previstos por la Empresa, se procederá a comprobar que dichos soportes se pueden leer correctamente y restaurarse sin problemas. Para ello se restaurará en una carpeta temporal el backup completo, comprobándose que el procedimiento de restauración y los datos del fichero son correctos. En caso de que el soporte fuera erróneo se sustituiría por el soporte del día anterior, siempre y cuando éste superara con éxito la correspondiente comprobación.

Todos los soportes utilizados por ***CHELO HISPANA, S.L.*** para la realización de las copias de backup se etiquetarán debidamente de conformidad con lo previsto en el presente Documento de Seguridad.

Todos los soportes se guardarán en dispositivitos de almacenamiento con mecanismos que obstaculicen su apertura, permitiéndose únicamente el acceso al personal autorizado en el presente Documento de Seguridad.

Respecto a las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal (servidores de pre-producción) no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado. Cuando esté previsto realizar este tipo de pruebas con datos reales, será obligatorio realizar con carácter previo una copia de seguridad específica de los datos.

2. ***Procedimiento de recuperación***

El proceso de recuperación de datos llevará asociado una serie de actividades genéricas que se detallan en los siguientes apartados. Estas actividades se agrupan en las fases siguientes:

a) Detección de la pérdida de datos.
b) Aprobación de la recuperación de datos.
c) Recuperación de los datos.
d) Registro de la incidencia.

a) Detección de la pérdida de datos.

En cualquiera de las fases del tratamiento de los datos de carácter personal de ***CHELO HISPANA, S.L.*** puede existir una incidencia que ocasione una pérdida de datos. Todo aquel usuario que detecte una incidencia tiene la obligación de comunicarlo al Responsable de Seguridad o en quien éste delegue, para que se proceda al registro de la incidencia y se adopten las medidas de restauración de los datos oportunas.

b) Aprobación de la recuperación de datos.

El Responsable de Seguridad deberá comprobar la pérdida de los datos y aprobar el procedimiento de restauración de los mismos.

Únicamente en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo de la restauración de los datos, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el Registro de Incidencias de la Empresa.

c) Recuperación de los datos

El Responsable de Seguridad y por delegación de éste el administrador del sistema afectado deberán identificar el día a restaurar, en función de las copias de respaldo disponibles con fecha anterior a la incidencia.

Una vez identificado el soporte o cinta a restaurar, se realizará la recuperación de los datos.

d) Registro de la incidencia

El Responsable de Seguridad deberá asegurarse de que la incidencia se registra según el Procedimiento de Gestión de Incidencias.

CHELO HISPANA, S.L.

REGISTRO DE ACCESOS A DOCUMENTACIÓN

REGISTRO DE ACCESOS A DOCUMENTACIÓN

El acceso a la documentación que contenga datos de carácter personal de nivel alto se limitará exclusivamente al personal autorizado. Para el caso de documentos que puedan ser utilizados por múltiples usuarios, ***CHELO HISPANA, S.L.*** dispone del presente Registro de Accesos a los efectos de identificar los accesos realizados.

REGISTRO DE ACCESOS A DOCUMENTACIÓN

HOJA DE REGISTRO DE ACCESO A DOCUMENTACIÓN EN PAPEL			
Fecha:		**Hora:**	
Solicita el acceso:			
Autoriza el acceso:			
Fichero Accedido:			
Motivo del Acceso:			
Firma:			
Hoja de acceso nº 1			

REGISTRO DE ACCESOS A DOCUMENTACIÓN

HOJA DE REGISTRO DE ACCESO A DOCUMENTACIÓN EN PAPEL			
Fecha:		**Hora:**	
Solicita el acceso:			
Autoriza el acceso:			
Fichero Accedido:			
Motivo del Acceso:			
Firma:			
Hoja de acceso nº 2			

REGISTRO DE ACCESOS A DOCUMENTACIÓN

HOJA DE REGISTRO DE ACCESO A DOCUMENTACIÓN EN PAPEL			
Fecha:		**Hora:**	
Solicita el acceso:			
Autoriza el acceso:			
Fichero Accedido:			
Motivo del Acceso:			
Firma:			
Hoja de acceso nº 3			

REGISTRO DE ACCESOS A DOCUMENTACIÓN

HOJA DE REGISTRO DE ACCESO A DOCUMENTACIÓN EN PAPEL			
Fecha:		**Hora:**	
Solicita el acceso:			
Autoriza el acceso:			
Fichero Accedido:			
Motivo del Acceso:			
Firma:			
Hoja de acceso nº 4			

REGISTRO DE ACCESOS A DOCUMENTACIÓN

HOJA DE REGISTRO DE ACCESO A DOCUMENTACIÓN EN PAPEL			
Fecha:		**Hora:**	
Solicita el acceso:			
Autoriza el acceso:			
Fichero Accedido:			
Motivo del Acceso:			
Firma:			
Hoja de acceso nº 5			

REGISTRO DE ACCESOS A DOCUMENTACIÓN

HOJA DE REGISTRO DE ACCESO A DOCUMENTACIÓN EN PAPEL			
Fecha:		**Hora:**	
Solicita el acceso:			
Autoriza el acceso:			
Fichero Accedido:			
Motivo del Acceso:			
Firma:			
Hoja de acceso nº 6			

CHELO HISPANA, S.L.

REGISTRO DE AUTORIZACIONES

REGISTRO DE AUTORIZACIONES

Las autorizaciones emitidas por las personas habilitadas al efecto por parte del Responsable de los Ficheros son registradas haciéndose constar el tipo de autorización, la fecha y la hora en que se ha otorgado, la persona que emite la Autorización, el usuario o perfil de usuario a quién se autoriza, así como el periodo de vigencia de la autorización.

También deberán constar en el presente Libro Registro de Autorizaciones aquellas autorizaciones otorgadas a los Encargados del Tratamiento que, para la prestación del servicio contratado, requieran trabajar con los datos personales fuera de los locales del propio encargado del tratamiento.

EJEMPLO:

HOJA DE AUTORIZACIÓN					
Nº de Autorización:	1/2008	**Fecha:**	15/04/2008	**Hora:**	09:00
Tipo de Autorización					
Autorización para conceder, alterar o anular el acceso a los distintos recursos de los sistemas de información.					
Persona que emite la Autorización					
Responsable de Seguridad:					
Usuario o perfil de usuario a quien se autoriza					
Personal del Dpto. de Atención al Público					
Periodo de vigencia:	Indefinido. Temporal. De __/__/____ a __/__/____				
Firmas:					
Hoja de autorización nº 1					

REGISTRO DE AUTORIZACIONES

HOJA DE AUTORIZACIÓN					
Nº de Autorización:		**Fecha:**		**Hora:**	
Tipo de Autorización					
Persona que emite la Autorización					
Usuario o perfil de usuario a quien se autoriza					
Periodo de vigencia:	Indefinido. Temporal. De __/__/____ a __/__/____				
Firmas:					
Hoja de autorización nº 2					

REGISTRO DE AUTORIZACIONES

HOJA DE AUTORIZACIÓN					
Nº de Autorización:		**Fecha:**		**Hora:**	
Tipo de Autorización					
Persona que emite la Autorización					
Usuario o perfil de usuario a quien se autoriza					
Periodo de vigencia:	Indefinido. Temporal. De __/__/____ a __/__/____				
Firmas:					
Hoja de autorización nº 3					

REGISTRO DE AUTORIZACIONES

HOJA DE AUTORIZACIÓN					
Nº de Autorización:		**Fecha:**		**Hora:**	
Tipo de Autorización					
Persona que emite la Autorización					
Usuario o perfil de usuario a quien se autoriza					
Periodo de vigencia:	Indefinido. Temporal. De __/__/____ a __/__/____				
Firmas:					
Hoja de autorización nº 4					

REGISTRO DE AUTORIZACIONES

HOJA DE AUTORIZACIÓN					
Nº de Autorización:		**Fecha:**		**Hora:**	
Tipo de Autorización					
Persona que emite la Autorización					
Usuario o perfil de usuario a quien se autoriza					
Periodo de vigencia:	Indefinido. Temporal. De __/__/____ a __/__/____				
Firmas:					
Hoja de autorización nº 5					

REGISTRO DE AUTORIZACIONES

HOJA DE AUTORIZACIÓN					
Nº de Autorización:		**Fecha:**		**Hora:**	
Tipo de Autorización					
Persona que emite la Autorización					
Usuario o perfil de usuario a quien se autoriza					
Periodo de vigencia:	Indefinido. Temporal. De __/__/____ a __/__/____				
Firmas:					
Hoja de autorización nº 6					

CHELO HISPANA, S.L.

REGISTRO DE
ENTRADA DE SOPORTES

REGISTRO DE ENTRADA DE SOPORTES

En el presente registro se anotan todas las entradas que se produzcan de soportes y documentos que contengan datos de carácter personal de nivel medio en las oficinas e instalaciones de ***CHELO HISPANA, S.L.***. El presente registro, mediante la inclusión de la firma del Responsable de Seguridad, servirá a modo de autorización de la persona responsable de la recepción.

HOJA DE ENTRADA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de entrada:	
Emisor:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la recepción:	
Firma responsable:	
Hoja de entrada de soporte nº 1	

HOJA DE ENTRADA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de entrada:	
Emisor:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la recepción:	
Firma responsable:	
Hoja de entrada de soporte nº 2	

HOJA DE ENTRADA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de entrada:	
Emisor:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la recepción:	
Firma responsable:	
Hoja de entrada de soporte nº 3	

HOJA DE ENTRADA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de entrada:	
Emisor:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la recepción:	
Firma responsable:	
Hoja de entrada de soporte nº 4	

HOJA DE ENTRADA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de entrada:	
Emisor:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la recepción:	
Firma responsable:	
Hoja de entrada de soporte nº 5	

HOJA DE ENTRADA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de entrada:	
Emisor:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la recepción:	
Firma responsable:	
Hoja de entrada de soporte nº 6	

CHELO HISPANA, S.L.

REGISTRO DE SALIDA DE SOPORTES

REGISTRO DE SALIDA DE SOPORTES

En el presente registro se anotan todas las salidas de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control de ***CHELO HISPANA, S.L.***. El presente registro, mediante la inclusión de la firma del Responsable de Seguridad, servirá a modo de autorización de salida de soportes y documentos, así como autorización de la persona responsable de la entrega.

HOJA DE SALIDA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de salida:	
Destinatario:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la entrega:	
Firma responsable:	
Hoja de salida de soporte nº 1	

HOJA DE SALIDA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de salida:	
Destinatario:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la entrega:	
Firma responsable:	
Hoja de salida de soporte nº 2	

HOJA DE SALIDA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de salida:	
Destinatario:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la entrega:	
Firma responsable:	
Hoja de salida de soporte nº 3	

HOJA DE SALIDA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de salida:	
Destinatario:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la entrega:	
Firma responsable:	
Hoja de salida de soporte nº 4	

HOJA DE SALIDA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de salida:	
Destinatario:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la entrega:	
Firma responsable:	
Hoja de salida de soporte nº 5	

HOJA DE SALIDA DE SOPORTES	
Tipo y Nº de documentos y soportes:	
Fecha y hora de salida:	
Destinatario:	
Tipo de información contenida:	
Forma de envío:	
Responsable de la entrega:	
Firma responsable:	
Hoja de salida de soporte nº 6	

CHELO HISPANA, S.L.

REGISTRO DE INCIDENCIAS

GESTIÓN DE INCIDENCIAS. AUTORIZACIONES DE RECUPERACIÓN DE DATOS

Las incidencias en relación con los ficheros que contengan datos de carácter personal son registradas haciéndose constar el tipo de incidencia, la fecha y la hora en que se ha producido o detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. En caso de pérdida o alteración de datos de carácter personal de nivel medio o alto también se registrará el procedimiento utilizado para recuperar los datos, así como la persona que ejecutó el proceso de recuperación, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

GESTIÓN DE INCIDENCIAS. AUTORIZACIONES DE RECUPERACIÓN DE DATOS

HOJA DE INCIDENCIA					
Nº de Incidencia:		**Fecha:**		**Hora:**	
Tipo de Incidencia					
Efectos					
Medidas Correctoras aplicadas					
Precedimiento de recuperación de datos					
Datos restaurados					
Datos restaurados o grabados manualmente					
Persona que notifica la incidencia					
Persona a quien se notifica la incidencia					
Persona que realiza la restauración					
Responsable del fichero					
Firma:					
Hoja de incidencia nº 1					

GESTIÓN DE INCIDENCIAS. AUTORIZACIONES DE RECUPERACIÓN DE DATOS

HOJA DE INCIDENCIA					
Nº de Incidencia:		**Fecha:**		**Hora:**	
Tipo de Incidencia					
Efectos					
Medidas Correctoras aplicadas					
Precedimiento de recuperación de datos					
Datos restaurados					
Datos restaurados o grabados manualmente					
Persona que notifica la incidencia					
Persona a quien se notifica la incidencia					
Persona que realiza la restauración					
Responsable del fichero					
Firma:					
Hoja de incidencia nº 2					

GESTIÓN DE INCIDENCIAS. AUTORIZACIONES DE RECUPERACIÓN DE DATOS

HOJA DE INCIDENCIA					
Nº de Incidencia:		**Fecha:**		**Hora:**	
Tipo de Incidencia					
Efectos					
Medidas Correctoras aplicadas					
Precedimiento de recuperación de datos					
Datos restaurados					
Datos restaurados o grabados manualmente					
Persona que notifica la incidencia					
Persona a quien se notifica la incidencia					
Persona que realiza la restauración					
Responsable del fichero					
Firma:					
Hoja de incidencia nº 3					

GESTIÓN DE INCIDENCIAS. AUTORIZACIONES DE RECUPERACIÓN DE DATOS

HOJA DE INCIDENCIA					
Nº de Incidencia:		**Fecha:**		**Hora:**	
Tipo de Incidencia					
Efectos					
Medidas Correctoras aplicadas					
Precedimiento de recuperación de datos					
Datos restaurados					
Datos restaurados o grabados manualmente					
Persona que notifica la incidencia					
Persona a quien se notifica la incidencia					
Persona que realiza la restauración					
Responsable del fichero					
Firma:					
Hoja de incidencia nº 4					

GESTIÓN DE INCIDENCIAS. AUTORIZACIONES DE RECUPERACIÓN DE DATOS

HOJA DE INCIDENCIA					
Nº de Incidencia:		**Fecha:**		**Hora:**	
Tipo de Incidencia					
Efectos					
Medidas Correctoras aplicadas					
Precedimiento de recuperación de datos					
Datos restaurados					
Datos restaurados o grabados manualmente					
Persona que notifica la incidencia					
Persona a quien se notifica la incidencia					
Persona que realiza la restauración					
Responsable del fichero					
Firma:					
Hoja de incidencia nº 5					

GESTIÓN DE INCIDENCIAS. AUTORIZACIONES DE RECUPERACIÓN DE DATOS

HOJA DE INCIDENCIA					
Nº de Incidencia:		**Fecha:**		**Hora:**	
Tipo de Incidencia					
Efectos					
Medidas Correctoras aplicadas					
Precedimiento de recuperación de datos					
Datos restaurados					
Datos restaurados o grabados manualmente					
Persona que notifica la incidencia					
Persona a quien se notifica la incidencia					
Persona que realiza la restauración					
Responsable del fichero					
Firma:					
Hoja de incidencia nº 6					

ENCARGADOS

REGISTRO DE TRATAMIENTO DE DATOS POR CUENTA DE TERCEROS

De conformidad con lo establecido en el artículo 82 del RD 1720/2007, a continuación se identifican los tratamientos de datos efectuados por terceros sobre los ficheros titularidad de la Empresa

Identidad del Encargado del Tratamiento:	**GESTIÓN LUCENA S.L.**			
Lugar y forma de realización del tratamiento: (Marque con una X la opción correcta)				
En los locales de la Empresa	**En los locales del Encargado del Tratamiento**	**De forma remota, sin que los datos puedan incorporarse a sistemas o soportes distintos de los de la Empresa**	**Fecha firma Contrato**	**Vigencia del encargo(Indefinida/fecha finalzación)**
X	**X**			

Ficheros tratados	**Medidas de seguridad**
"Clientes" "Proveedores"	**BÁSICO BASICO**

ENCARGOS

REGISTRO DE TRATAMIENTO DE DATOS POR CUENTA DE TERCEROS

De conformidad con lo establecido en el artículo 88.5 del RD 1720/2007, a continuación se identifican los ficheros tratados por la Empresa en concepto de Encargado del Tratamiento, con referencia expresa al contrato que regula las condiciones de cada encargo, el nivel de las medidas de seguridad a implantar, el período de vigencia y la identificación de los responsables.

Responsable de los ficheros	Fecha Firma Contrato	Vigencia del Encargo

EQUIPOS				
Equipo	Marca	Procesador	Memoria	Disco Duro
Terminal Fijo 1				
Terminal Portatil 1				
Terminal Portatil 2				

PRESTADORES SERVICIOS SIN ACCESO A DATOS

Identidad de la Prestadora de Servicios	CIF
SECURITAS DIRECT ESPANA, SA	A26106013